# Voluntary Voting System Guidelines Overview

This section provides an overview of the Voluntary Voting System Guidelines (VVSG), Version 1. The VVSG was created in response to the Help America Vote Act (HAVA) of 2002 and is based on the initial set of recommendations of the Technical Guidelines Development Committee (TGDC) mandated by HAVA. The VVSG Version 1 augments the Voting Systems Standard (VSS) of 2002 (VSS-2002), which was promulgated by the Federal Election Commission (FEC). This overview serves as an explanation of how the VVSG Version 1 differs from the VSS-2002 and provides a basis for further improvements. In addition, it provides a high level overview of the major sections of the two volumes that make up VVSG Version 1.

## Background

The Help America Vote Act (HAVA) established the Technical Guidelines Development Committee to assist the Election Assistance Commission (EAC) with the development of voluntary voting system guidelines. HAVA directs the National Institute of Standards and Technology (NIST) to chair the TGDC and to provide technical support to the TGDC in the development of these guidelines. The TGDC's initial set of recommendations for these guidelines were presented to the Election Assistance Commission in May 2005, in accordance with HAVA's nine-month deadline.

VVSG Version 1 is intended to assist States election officials in preparing for the 2006 election. This document augments the VSS-2002 to address the critical areas of accessibility, usability and computer security. In addition, the VVSG includes an improved glossary to promote common understanding, a conformance clause, and an updated Appendix on error rates.

It is important to note that the VVSG Version 1 is only an interim set of guidelines. The EAC is working with both the TGDC and NIST to create a redesigned VVSG (called VVSG Version 2) that will address a large range of issues including rewriting the requirements, if necessary, to make them more precise and testable and further addressing key human factors and computer security issues. The new requirements affect the basic design of voting systems to such a degree that these types of changes cannot reasonably be made and tested in time for the 2006 election cycle.

## Brief History of Voting Systems Standards and Guidelines

In 1975, the National Bureau of Standards (now the National Institute of Standards and Technology) and the Office of the Federal Elections (the Office of Election Administration's predecessor at the General Accounting Office) produced a joint report, *Effective Use of Computing Technology in Vote Tallying.* This report concluded that a basic cause of computer-related election problems was the lack of appropriate technical skills at the state and local level to develop or implement sophisticated Standards against which voting system hardware and software could be tested. A subsequent Congressionally-authorized study produced by the FEC and the National Bureau of Standards detailed the need for a federal agency to develop national

performance Standards that could be used as a tool by state and local election officials in the testing, certification, and procurement of computer-based voting systems.

In 1984, Congress appropriated funds for the FEC to develop voluntary national Standards for computer-based voting systems. The FEC formally approved the *Performance and Test Standards for Punchcard, Marksense and Direct Recording Electronic Voting Systems* in January 1990. This document is generally referred to as the *Voting Systems Standards, or 1990 VSS.*

The national testing effort was developed and overseen by the National Association of State Election Director's Voting Systems Board, which is composed of election officials and independent technical advisors. NASED's testing program was initiated in 1994 and more than 30 voting systems or components of voting systems have gone through the (NASED's) testing and qualification process. In addition, many systems have subsequently been certified at the state level using the Standards in conjunction with functional and technical requirements developed by state and local policymakers to address the specific needs of their jurisdictions.

As the qualification process matured and qualified systems were used in the field, the Voting Systems Board, in consultation with the testing labs, was able to identify certain testing issues that needed to be resolved. Moreover, rapid advancements in information and personal computer technologies introduced new voting system development and implementation scenarios not contemplated by the 1990 Standards.

In 1997, NASED briefed the FEC on the necessity for continued FEC involvement, citing the importance of keeping the Standards current in its reflection of modern and emerging technologies employed by voting system vendors. Following a Requirements Analysis released in 1999, the Commission authorized the Office of Election Administration to revise the Standards to reflect contemporary needs of the elections community. This resulted in the 2002 Voting Systems Standards.

In 2002, Congress passed HAVA, which created a new process for improving voluntary voting system guidelines. A new federal entity was created, the Election Assistance Commission, to oversee the process. The EAC established the Technical Guidelines Development Committee in accordance with the requirements of section 221 of HAVA pursuant to the Federal Advisory Committee Act, 5 U.S.C. App. 2. The TGDC's objectives and duties were to act in the public interest to assist the EAC in the development of the voluntary voting system guidelines. The membership, as defined by HAVA, includes:

- The Director of the National Institute of Standards and Technology (NIST) who shall serve as its chair,
- Members of the Standards Board,
- Members of the Board of Advisors,
- Members of the Architectural and Transportation Barrier, and Compliance Board (Access Board),
- A representative of the American National Standards Institute,
- A representative of the IEEE,
- Two representatives of the NASED selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party, and

- Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

The TGDC first met in July 2004 and delivered its initial set of recommendations to the EAC in April 2005. The initial set of recommendations augments the VSS-2002 by including security measures for auditability, wireless communications and software distribution and setup, and improvements for the accessibility guidelines and usability design guidelines . The TGDC also recommended that the VSS-2002 should be replaced with a far-reaching guideline that would address in-depth security, performance-based guidelines for usability testing and an overhaul of the standards and test methods to meet today's more rigorous needs for electronic voting systems.

## Issues Addressed by the VVSG Version 1

The VVSG Version 1 adds or significantly changes eight technical topics of the VSS-2002. In addition, there are three organizational changes in the new sections. All other material remains the same.

### Conformance Clause

The VSS-2002 did not include a conformance clause. A new one has been written and inserted as Section 1.7. The previous material in Section 1.7, the Outline, has been moved to 1.8.

Conformance is defined as the fulfillment by a product, process, or service of requirements as specified in a standard or specification. Conformance testing is the determination of whether an implementation (i.e., product, process, or service) faithfully satisfies the requirements and thus, conforms.

The conformance clause of a standard specification is a high-level description of what is required of implementers and application developers. It, in turn, refers to other parts of the standard. The conformance clause may specify minimal requirements for certain functions and minimal requirements for implementation-dependent values. It may also specify the permissibility of extensions, options, and alternative approaches and how they are to be handled.

### Human Factors

In the VSS-2002, Section 2.2.7 addressed Accessibility and Section 3.4.9 addressed Human Engineering—Controls and Displays. The VSS-2002 also contained Appendix C on Usability and two NASED Technical Guides (Guide #1 and Guide #2). The VVSG Version 1 replaces all of those items with a new Section 2.2.7 that addresses Human Factors including accessibility, usability and limited English proficiency. The section improves the design specifications. Future versions of the VVSG will contain performance-based requirements.

### Security Overview

A new security section was added as Section 6.0. It contains four parts: an Overview and three chapters of security requirements. The section was added to explain the VVSG approach to security. In summary, future versions of the VVSG will require independent verification. There are many ways known today to achieve independent verification and more ways may be developed. Current methods include dual process systems, witness systems, cryptographic-based

systems, optical scan systems, and paper audit trails. The overview provides only preliminary high level requirements. This is a new area in voting systems and it is expected to evolve significantly in VVSG Version 2. The Security Overview is an informative (non-normative) section of the VVSG Version 1. Requirements for voter verified paper audit trail systems, which are a type of independent verification system, are specified in their own section. Version 2 of the VVSG will have complete requirements for at least three additional methods.

**Voter Verified Paper Audit Trails**

The VSS-2002 contained no requirements for voter verified paper audit trails. The VVSG Version 1 is providing requirements for voter verified paper audit trails (VVPAT) so that States that choose to implement VVPAT or States that are considering implementation can utilize these requirements to help ensure the effective operation of these systems. The EAC, TGDC, and NIST are taking no position with respect to the implementation of VVPAT systems and are neither requiring nor endorsing voter verified paper audit trails. Methods other than VVPAT can provide ways to achieve independent verification. These other methods are described in the Security Overview.

**Wireless Technology**

The TGDC concluded that the use of wireless technology introduces risk and should be approached with caution. Therefore, the VVSG Version 1 includes a special section on wireless that augments the general telecommunications guidelines in Section 5. The VVSG Version 1 requires that wireless transmissions be encrypted to protect against a variety of security problems.

**Software Distribution and Setup Validation**

The VSS-2002 contains many requirements to help voting officials validate the software and the setup of voting system software and hardware. Subsequent to the publication of the VSS-2002, the EAC invited all voting software vendors to submit their software to a national software repository maintained by NIST. This section of the VVSG Version 1 builds on the VSS-2002 to include use of this repository and other validation mechanisms.

**Glossary**

This glossary contains terms from the VSS-2002 as well as the inclusion of additional terms needed to understand voting and related areas such as security, human factors, and testing. Each term includes a definition and its source as well as an association as to the domain for which the term applies. Having a common set of terminology forms the basis for understanding requirements and for discussing improvements. The glossary is also available in a web-based on-line version at http://www.nist.gov/votingglossary.

**Error Rates**

Volume II, Appendix C addresses error rates. This appendix contains revised procedures to test that systems meet the indicated error rates. These apply to errors introduced by the system, defined as a ballot position error rate, and not by a voter's action. Further research on human interface and usability issues is needed to enable the development of Standards for error rates that account for human error.

There were concerns about the VSS-2002 Appendix regarding the numbers listed in the probability ratio sequential test (PRST) of the Mean Time Before Failure (MTBF) that (1) the numbers do not correspond to the numbers for the same table in the 1990 VSS, even though the stated assumptions do not change, and (2) the numbers from neither the 1990 nor the 2002 tables correspond to numbers that would result from standard PRST formulas listed in standard references such as the military handbook MIL-HDBK-781A. To address these concerns, the revised Appendix has replaced the numbers in the table with those that would indicated by the truncated PRST design from MIL-HDBK-781A with the corresponding parameters and made it more clear in the text that a truncated design was chosen. Using standard theoretical formulas leads to somewhat different numbers, but the revised Appendix C uses numbers from the MIL-HDBK-781A because they may be considered more standard and produce a less drastic change.

Also, in the 1990 VSS, there was an appendix devoted to the definition and use of "partial failures." This appendix was eliminated from the VSS-2002. The new version eliminated the paragraph and diagram in Appendix C that used partial failures.

The new version also includes statements reminding users to be cognizant of the assumptions involved in tests that use time-based exponential failure times and constant failure rates. Given the concerns that have been stated about appropriate testing times, note that the given table is appropriate only for the stated parameters, and that officials should assess the appropriateness of whatever parameters are used in testing.

**Best Practices for Voting Officials**

The VSS-2002 contained requirements for voting systems and for testing entities. However, requirements for human factors, wireless communications, VVPAT, software distribution and setup validation depend not only on voting systems providing specific capabilities but on voting officials developing and carrying out appropriate procedures. Consequently, the VVSG Version 1 contains Best Practices for voting officials. The new sections define each requirement as pertaining to voting systems, test authorities, or voting officials. The requirements for voting officials are collected in Appendix C of Volume 1. (Appendix C had previously been Usability.)

**Process**

The VSS-2002 defined three major stages of voting: pre-voting, voting and post-voting. The stage for each requirement is marked in the new sections. The VVSG Version 2 will have a more detailed process model and will allow for finer granularity.

**Structure of Requirements**

The new sections of the VVSG Version 1 have a more structured approach to the requirements than that of the VSS-2002. Each requirement is numbered according to a hierarchical scheme in which higher-level requirements (such as "provide accessibility for blind voters") are supported by lower-level requirements ("provide an audio-tactile interface").

Some of these requirements are directly testable, and some not. The latter tend to be higher-level and are included because 1) they are testable *indirectly* insofar as their sub-requirements are testable, and 2) they often provide the structure and rationale for lower-level requirements.

In future versions of the VVSG, the testability of each requirement will be explicitly denoted, and test methods provided for each testable requirement.

**<u>Summary of Content of Volume I</u>**

Volume I contains performance standards for electronic components of voting systems. In addition to containing a glossary (Appendix A) and applicable references (Appendix B), Volume I is divided into nine sections:

- **Section 1- Introduction:** This section provides an introduction to the Standards, addressing the following topics:
    - Objectives and usage of the Standards;
    - Development history for initial Standards;
    - Update of the Standards;
    - Accessibility for individuals with disabilities;
    - Definitions of key terms;
    - Application of the Standards and test specifications
    - Conformance clause; and
    - Outline of contents.
- **Section 2 - Functional Capabilities:** This section contains Standards detailing the functional capabilities required of a voting system. This section sets out precisely what it is that a voting system is required to do. This section also sets forth the minimum actions a voting system must be able to perform to be eligible for qualification. For organizational purposes, functional capabilities are categorized by the phase of election activity in which they are required:
    - **Overall Capabilities**: These functional capabilities apply throughout the election process. They include security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunications, and data retention.
    - **Pre-voting Capabilities**: These functional capabilities are used to prepare the voting system for voting. They include ballot preparation, the preparation of election-specific software (including firmware), the production of ballots or ballot pages, the installation of ballots and ballot counting software (including firmware), and system and equipment tests.
    - **Voting Capabilities**: These functional capabilities include all operations conducted at the polling place by voters and officials including the generation of status messages.
    - **Post-voting Capabilities**: These functional capabilities apply after all votes have been cast. They include closing the polling place; obtaining reports by voting machine, polling place, and precinct; obtaining consolidated reports; and obtaining reports of audit trails.
    - **Maintenance, Transportation and Storage Capabilities**: These capabilities are necessary to maintain, transport, and store voting system equipment.

  For each functional capability, common standards are specified. In recognition of the diversity of voting systems, some of the standards have additional requirements that apply only if the system incorporates certain functions (for example, voting systems

employing telecommunications to transmit voting data) or configurations (for example, a central count component). Where system-specific standards are appropriate, common standards are followed by standards applicable to specific technologies (i.e., paper-based or DRE) or intended use (i.e., central or precinct count).

- **Section 3 - Hardware Standards:** This section describes the performance requirements, physical characteristics, and design, construction, and maintenance characteristics of the hardware and related components of a voting system. This section focuses on a broad range of devices used in the design and manufacture of voting systems, such as:
    - For paper ballots: printers, cards, boxes, transfer boxes, and readers;
    - For electronic systems: ballot displays, ballot recorders, precinct vote control units;
    - For voting devices: punching and marking devices and electronic recording devices;
    - Voting booths and enclosures;
    - Equipment used to prepare ballots, program elections, consolidate and report votes, and perform other elections management activities;
    - Fixed servers and removable electronic data storage media; and
    - Printers.

  The Standards specify the minimum values for the relevant attributes of hardware, such as:
    - Accuracy;
    - Reliability;
    - Stability under normal environmental operating conditions and when equipment is in storage and transit;
    - Power requirements and ability to respond to interruptions of power supply;
    - Susceptibility to interference from static electricity and magnetic fields;
    - Product marking; and
    - Safety.
- **Section 4- Software Standards:** This section describes the design and performance characteristics of the software embodied in voting systems, addressing both system level software and voting system application software. The requirements of this section are intended to ensure that the overall objectives of accuracy, logical correctness, privacy, system integrity, and reliability are achieved. Although this section emphasizes software, the software standards may influence hardware design in some voting systems.

  The requirements of this section apply to all software developed for use in voting systems, including:
    - Software provided by the voting system vendor and its component suppliers; and

- Software furnished by an external provider where the software is potentially used in any way during voting system operation.

The general standards in this section apply to software used to support the broad range of voting system activities, including pre-voting, voting and post-voting activities. System specific Standards are defined for ballot counting, vote processing, the creation of an unalterable audit trail, and the generation of output reports and files. Voting system software is also subject to the security requirements of Section 6.

- **Section 5 - Telecommunications Standards**: This section describes the requirements for the telecommunications components of voting systems. Additionally, it defines the acceptable levels of performance against these characteristics. For the purpose of the Standards, telecommunications is defined as the capability to transmit and receive data electronically regardless of whether the transmission is localized within the polling place or the data is transmitted to a geographically distinct location. The requirements in this section represent functional and performance requirements for the transmission of data that is used to operate the system and report official election results. Where applicable, this section specifies minimum values for critical performance and functional attributes involving telecommunications hardware and software components.

  This section addresses telecommunications hardware and software across a broad range of technologies such as dial-up communications technologies, high-speed telecommunications lines (public and private), cabling technologies, communications routers, modems, modem drivers, channel service units (CSU)/data service units (DSU), and dial-up networking applications software.

  Additionally, this section applies to voting-related transmissions over public networks, such as those provided by regional telephone companies and long distance carriers. This section also applies to private networks regardless of whether the network is owned and operated by the election jurisdiction. For systems that transmit data over public networks, this section applies to telecommunications components installed and operated at settings supervised by election officials, such as polling places or central offices.

- **Section 6 - Security Standards:** This section starts with a description of a new approach to securing voting systems called independent verification. The section introduces the concept of independent verification and explains several approaches for achieving it. The Security Section contains a new section on how to secure voter verified paper audit trail systems, but only has preliminary requirements for other independent verification approaches. Independent verification is not required in VVSG Version 1, but will be required in Version 2. There are new requirements for wireless technology and software distribution and setup. The remainder of the section is unchanged from VSS-2002 and describes the security capabilities for a voting system, encompassing the system's hardware, software, communications, and documentation. The requirements of this section recognize that no predefined set of security Standards will address and defeat all conceivable or theoretical threats. However, the Standards articulate requirements to achieve acceptable levels of integrity, reliability, and inviolability. Ultimately, the objectives of the security Standards for voting systems are to:

  - Establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized;

  - Protect the system from intentional manipulation and fraud;

- Protect the system from malicious mischief;
- Identify fraudulent or erroneous changes to the system; and
- Protect secrecy in the voting process.

These Standards are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, the Standards identify several types of risk that must be addressed, including:

- Unauthorized changes to system capabilities for defining ballot formats, casting and recording votes, calculating vote totals consistent with defined ballot formats, and reporting vote totals;
- Alteration of voting system audit trails;
- Altering a legitimately cast vote;
- Preventing the recording of a legitimately cast vote,
- Introducing data for a vote not cast by a registered voter;
- Changing calculated vote totals;
- Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

- **Section 7 - Quality Assurance:** In the Standards, quality assurance is a vendor function with associated practices that confirms throughout the system development and maintenance life-cycle that a voting system conforms with the Standards and other requirements of state and local jurisdictions. Quality assurance focuses on building quality into a system and reducing dependence on system tests at the end of the life-cycle to detect deficiencies.

  This section describes the responsibilities of the voting system vendor for designing and implementing a quality assurance program to ensure that the design, workmanship, and performance requirements of the Standards are achieved in all delivered systems and components. These responsibilities include:

  - Development of procedures for identifying and procuring parts and raw materials of the requisite quality, and for their inspection, acceptance, and control.
  - Documentation of hardware and software development processes.
  - Identification and enforcement of all requirements for in-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware, as well as installation and operation of software or firmware.
  - Procedures for maintaining all data and records required to document and verify the quality inspections and tests.

- **Section 8 - Configuration Management:** This section contains specific requirements for configuration management of voting systems. For the purposes of the Standards, configuration management is defined as a set of activities and associated practices that assures full knowledge and control of the components of a system, beginning with its initial development, progressing throughout its development and construction, and continuing with its ongoing maintenance and enhancement. This section describes activities in terms of their purpose and outcomes. It does not describe specific procedures or steps to be employed to accomplish them—these are left to the vendor to select.

  The requirements of this section address a broad set of record keeping, audit, and reporting activities that include:

  - Identifying discrete system components;
  - Creating records of formal baselines of all components;
  - Creating records of later versions of components;
  - Controlling changes made to the system and its components;
  - Submitting new versions of the system to Independent Test Authorities (ITA)s;
  - Releasing new versions of the system to customers;
  - Auditing the system, including its documentation, against configuration management records;
  - Controlling interfaces to other systems; and
  - Identifying tools used to build and maintain the system.

  Vendors are required to submit documentation of these procedures to the ITA as part of the Technical Data Package for system qualification testing. Additionally, as articulated in state or local election laws, regulations, or contractual agreements with vendors, authorized election officials or their representatives reserve the right to inspect vendor facilities and operations to determine conformance with the vendor's reported configuration management procedures.

- **Section 9 - Overview of Qualification Tests**: This section provides an overview for the qualification testing of voting systems. Qualification testing is the process by which a voting system is shown to comply with the requirements of the Standards and the requirements of its own design and performance specifications. The testing also evaluates the completeness of the vendor's developmental test program, including the sufficiency of vendor tests conducted to demonstrate compliance with stated system design and performance specifications, and the vendor's documented quality assurance and configuration management practices.

  The qualification test process is intended to discover errors that, should they occur in actual election use, could result in failure to complete election operations in a satisfactory manner. This section describes the scope of qualification testing, its applicability to voting system components, documentation that is must be submitted by the vendor, and the flow of the test process. This section also describes differences between the test

process for initial qualification testing of a system and the testing for modifications and re-qualification after a qualified system has been modified.

Since 1994, the testing described in this section has been performed by an ITA that is certified by NASED. For the future, HAVA provides for EAC-accredited testing authorities. HAVA tasks the Director of NIST to assist the EAC by recommending laboratories for EAC accreditation. NIST's National Voluntary Laboratory Accreditation Program (NVLAP) is developing a program to evaluate competent laboratories. While laboratories are being evaluated for recommendation by the Director, testing will continue to be done by the ITAs previously certified by NASED. The testing may be conducted by one or more ITAs for a given system, depending on the nature of tests to be conducted and the expertise of the certified ITA. The testing process involves the assessment of, but is not limited to:

- Absolute correctness of all ballot processing software, for which no margin for error exists;
- Operational accuracy in the recording and processing of voting data, as measured by the error rate articulated in Volume I, Section 3;
- Operational failure or the number of unrecoverable failures under conditions simulating the intended storage, operation, transportation, and maintenance environments for voting systems, using an actual time-based period of processing test ballots;
- System performance and function under normal and abnormal conditions; and
- Completeness and accuracy of the system documentation and configuration management records to enable purchasing jurisdictions to effectively install, test, and operate the system.

**Summary of Volume II Content**

- **Section 1 - Introduction:** This section provides an overview of Volume II, addressing the following topics:
  - The objectives of Volume II;
  - The general contents of Volume II;
  - The qualification testing focus;
  - The qualification testing sequence;
  - The evolution of testing; and
  - The outline of contents
- **Section 2 - Technical Data Package:** This section contains a description of vendor documentation relating to the voting system that shall be submitted with the system as a precondition for qualification testing. These items are necessary to define the product and its method of operation; to provide the vendor's technical and test data supporting the

its claims of the system's functional capabilities and performance levels; and to document instructions and procedures governing system operation and field maintenance.

The content of the Technical Data Package (TDP) shall contain a complete description of the following information about the system:

- Overall system design, including subsystems, modules, and interfaces;
- Specific functional capabilities;
- Performance and design specifications;
- Design constraints and compatibility requirements;
- Personnel, equipment, and facilities necessary for system operation, maintenance, and logistical support;
- Vendor practices for assuring system quality during the system's development and subsequent maintenance; and
- Vendor practices for managing the configuration of the system during development and for modifications to the system throughout its life-cycle.

- **Section 3 - Functionality Testing:** This section contains a description of the testing to be performed by the ITA to confirm the functional capabilities of a voting system submitted for qualification testing. It describes the scope and basis for functional testing, the general sequence of tests within the overall test process, and provides guidance on testing for accessibility. It also discusses testing of functionality of systems that operate on personal computers.

- **Section 4 - Hardware Testing:** This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the hardware components of a voting system submitted for qualification testing. This section requires ITAs to design and perform procedures that test the voting system hardware for both operating and non-operating environmental tests.

  Hardware testing begins with non-operating tests that require the use of an environmental test facility. These are followed by operating tests that are performed partly in an environmental facility and partly in a standard test laboratory or shop environment. The non-operating tests are intended to evaluate the ability of the system hardware to withstand exposure to various environmental conditions incidental to voting system storage, maintenance, and transportation. The procedures are based on test methods contained in Military Standards (MIL-STD) 810D, modified where appropriate, and include such tests as: bench handling, vibration, low and high temperature, and humidity.

  The operating tests involve running the system for an extended period of time under varying temperatures and voltages. This ensures that the hardware meets or exceeds the minimum requirements for reliability, data reading, and processing accuracy contained in Section 3 of Volume I. Although the procedure emphasizes equipment operability and data accuracy, it is not an exhaustive evaluation of all system functions. Moreover, the severity of the test conditions has in most cases been reduced from that specified in the Military Standards to reflect commercial, rather than military, practice.

- **Section 5 - Software Testing:** This section contains a description of the testing to be performed by the ITAs to confirm the proper functioning of the software components of a

voting system submitted for qualification testing. It describes the scope and basis for software testing, the initial review of documentation to support software testing, and the review of voting system source code.

The software qualification tests encompass a number of interrelated examinations. The examinations include selective review of source code for conformance with the vendor's stated standards, and other system documentation provided by the vendor. The code inspection is complemented by a series of functional tests to verify the proper performance of all system functions controlled by the software.

- **Section 6 - System Level Integration Testing:** This section contains a description of the testing conducted by the ITAs to confirm the proper functioning of the fully integrated components of a voting system submitted for qualification testing. It describes the scope and basis for integration testing, testing of internal and external system interfaces, testing of security capabilities, testing of accessibility features, and the configuration audits, including the evaluation of claims made in the system documentation.

  System-level qualification tests address the integrated operation of hardware, software and telecommunications capabilities (where applicable) to assess the system's response to a range of both normal and abnormal conditions in an attempt to compromise the system.

- **Section 7 - Examination of Vendor Practices for Configuration Management and Quality Assurance:** This section contains a description of examinations conducted by the ITAs to evaluate the extent to which vendors meet the requirements for configuration management and quality assurance. It describes the scope and basis for the examinations and the general sequence of the examinations. It also provides guidance on the substantive focus of the examinations.

  In reviewing configuration management practices, the ITAs examine the vendor's:
  - configuration management policy;
  - configuration identification policy;
  - baseline, promotion and demotion procedures;
  - configuration control procedures;
  - release process and procedures; and
  - configuration audit procedures.

  In reviewing quality assurance practices, the ITAs examine the vendor's:
  - quality assurance policy;
  - parts and materials tests and examinations;
  - quality conformance plans, procedures and inspection results; and
  - voting system documentation.